One rig to control them all

CHRIS HEUNEN, University of Edinburgh, United Kingdom
ROBIN KAARSGAARD, University of Southern Denmark, Denmark
LOUIS LEMONNIER, University of Edinburgh, United Kingdom

We introduce a theory for computational control, consisting of eight naturally interpretable equations. Adding these to a prop of base circuits constructs controlled circuits, borne out in examples of reversible Boolean circuits and quantum circuits. We prove that this syntactic construction semantically corresponds to taking the free rig category on the base prop.

This is an extended abstract of a more detailed preprint available on the arXiv [23].

1 INTRODUCTION

Many computations contain *controlled* commands, that is, commands that are executed depending on the value of some memory cell. By *control* we mean the aspects of a computation that govern these dependencies.[1] Typically, the controlled command acts on one part of memory, and the controlling memory cell resides in another part of memory. To be more precise, for example, consider controlled negation in reversible Boolean circuits: the target bit is flipped depending on the value of the control bit. The goal of this article is to identify, separate, and study in isolation, this notion of computational control.

Traditional control flow or data flow is often mixed up with other computational aspects of circuits. For example, in reversible Boolean or quantum circuits, multi-controlled gates such as the Toffoli gate are integral to universality and not treated differently than other, uncontrolled, gates [33]. Yet separating out the controlled aspects of a computation as specified by a circuit has several benefits.

(i) Multi-controlled gates are of foundational importance in many computational theories, including Boolean logic [34], reversible computation [32, 33], and quantum computation [29]. Isolating their control logic can help to better *understand* these theories.
(ii) In quantum hardware, (multi-)controlled gates are among the most costly ones to perform physically [4, 12, 36]. Separating out the control aspects can help find better optimisation strategies [3]. In general, partitioning off control aspects can help to *optimise* computations in a generic way that is independent of the 'base circuit theory' and therefore more efficient to apply.
(iii) Several recent results about logical completeness for quantum computation rely on elaborate families of equations [5, 6, 13–17, 20, 26]. Cordoning off control aspects can *simplify*, and thereby clarify the core status of some and make them more modular.

This article addresses these three challenges by introducing a theory of control governed by a handful of equations (see Figure 1). We argue that these equations completely capture control as follows.

(i) The equations have clear computational interpretations, and several have appeared in the literature before [28, 32]. Additionally, we show that the equations are canonical in a strong way, by relating them to the natural mathematical notion of a *rig category* [25, 35].

[1] We do not mean 'control theory' as used in e.g. engineering [19].

Authors' addresses: Chris Heunen, School of Informatics, University of Edinburgh, Edinburgh, EH8 9AB, United Kingdom, chris.heunen@ed.ac.uk; Robin Kaarsgaard, University of Southern Denmark, Odense, Denmark, kaarsgaard@imada.sdu.dk; Louis Lemonnier, School of Informatics, University of Edinburgh, Edinburgh, EH8 9AB, United Kingdom, louis.lemonnier@ed.ac.uk.

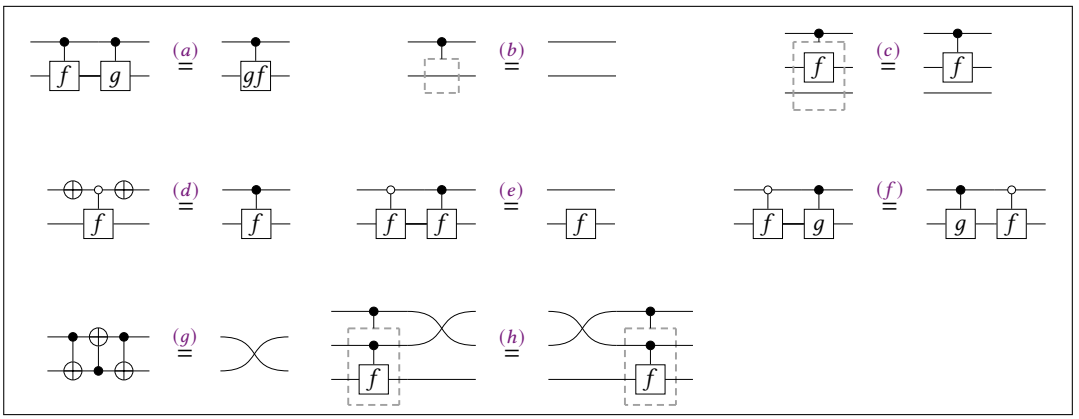


Fig. 1. Control equations.

Starting with an arbitrary 'base circuit theory', we syntactically construct a new 'controlled circuit theory'. We do this in the most general setting possible, using *prop*s [8, 21, 27]. The construction has a universal property: roughly, the controlled prop is the free rig category on the base prop. This is borne out in examples: starting with the circuit theory consisting of a single NOT gate, the controlled theory is universal for reversible Boolean circuits. Starting with an additional Hadamard gate, the controlled theory is universal for quantum circuits [30]. Starting with a single $\sqrt{X}$ gate in fact suffices for the latter [24].

(ii) The coherence theorems for rig categories [25, 35], and the fact that the control theory (of Figure 1) consists of only eight unquantified equations, give rise to many optimisation strategies. For example, we will show that the control theory suffices to syntactically derive equations like the following Sleator-Weinfurter decomposition quickly, that were before only known to hold semantically via matrix calculations in special cases [10, 31] (see Figure 2).

(iii) The equations simplify related work. The first works on complete equational theories for quantum circuits [13–15] contain a notion of *structural* equations, without a mathematical account of this notion. The same holds for [5, 6, 26]. Similarly, [18] defines the notion of controlled prop without relating it to any mathematical structure, while it is similarly not clear in [32] whether the template-based rewrite rules for control are complete. This article fills that gap by showing that the structure of control is exactly that of rig categories. Our work similarly structures and elucidates a line of research on quantum programming languages taking semantics in rig categories [9–11, 20, 22]. Finally, our results obviate work on circumventing no-control theorems by restricting to specific gate sets [7].

These results also substantiate the claim in the title, that rig structure encapsulates controlled computation, and only controlled computation. Thus rig categories form the bare minimum model of computation: the ability to compose instructions sequentially (with $\circ$), to consider data in parallel (with $\otimes$), and to use one piece of data to condition computations on another (using $\oplus$). This may also explain the ubiquity of matrices.

2 CONTROLLED PROPS

A *controllable prop* $(\mathbf{P}, +, 0, x)$, or *crop* for short, is a prop $(\mathbf{P}, +, 0)$ whose morphisms are endomorphisms and in which one morphism $x\colon 1 \longrightarrow 1$ is a distinguished involution. We sometimes refer to

this involution as the *NOT gate*. One important example of controllable prop is the prop **X** generated only by the NOT gate x.

Definition 1 (Controlled prop)**.** Given a controllable prop $(\mathbf{P}, +, 0, x)$, we extend it to a new prop with endofunctors C^0 and C^1 such that if $f\colon n \to n$, then $C^b(f)\colon 1+n \to 1+n$, and that, for all n and $f, f_1, f_2\colon n \to n$, we have equations:

(a) composition: $C^1(g \circ f) = C^1(g) \circ C^1(f)$;
(b) identity: $C^1(\mathrm{id}_n) = \mathrm{id}_{n+1}$;
(c) strength: $C^1(f + \mathrm{id}_m) = C^1(f) + \mathrm{id}_m$;
(d) colour change: $(x + \mathrm{id}_n) \circ C^0(f) \circ (x + \mathrm{id}_n) = C^1(f)$;
(e) complementarity: $C^0(f) \circ C^1(f) = \mathrm{id}_1 + f$;
(f) commutativity: $C^0(f_1) \circ C^1(f_2) = C^1(f_2) \circ C^0(f_1)$;
(g) "swap": $C^1(x) \circ \mathrm{swap}_{1,1} \circ C^1(x) \circ \mathrm{swap}_{1,1} \circ C^1(x) = \mathrm{swap}_{1,1}$;
(h) "swap" coherence: $(\mathrm{swap}_{1,1} \otimes \mathrm{id}_n) \circ C^1(C^1(f)) = C^1(C^1(f)) \circ (\mathrm{swap}_{1,1} \otimes \mathrm{id}_n)$.

Figure 1 gives a diagrammatic account of the above equations. Write **cP** for this new prop, that we call the *controlled prop* of **P**. Note that $(\mathbf{cP}, +, 0, x)$ is itself a controllable prop.

Theorem 2. *The controlled prop* **cX** *of* **X** *generated by a single involution is crop isomorphic to* $\mathbf{Perm}_2$.

To prove this, we define functors in both directions and show that they are inverse of each other. The direction $\mathbf{Perm}_2 \to \mathbf{cX}$ makes use of Gray code transpositions, which, like transpositions, generate all permutations.

3 RIGGED PROPS THANKS TO KRONECKER

In the context of matrices, the Kronecker product can be computed with direct sums only. Given a matrix M, the matrix $I_n \otimes M$ is obtained as the block-diagonal matrix $M \oplus \cdots \oplus M$. This hints at the fact that any theory around the direct sum can simulate the one of a tensor product, given some more coherence. To this effect, given a controllable prop $(\mathbf{P}, +, 0, x)$ with a set of generators G, and a set of relations R, we introduce its *rigged crop* $(\overline{\mathbf{P}}, \oplus, 0)$, as the prop generated by:

$$\overline{G} = \left\{\overline{g}\colon 2^k \to 2^l \;\middle|\; g\colon k \to l \in G\right\} \tag{1}$$

with equations

$$\overline{R} = \left\{\overline{f + \mathrm{id}} \circ \overline{\mathrm{id} + h} = \overline{\mathrm{id} + h} \circ \overline{f + \mathrm{id}} \;\middle|\; f, h \in G\right\} \tag{2}$$

$$\cup \left\{\overline{f} = \overline{h} \;\middle|\; (f = h) \in R\right\} \tag{3}$$

$$\cup \left\{\overline{x} = \gamma_{1,1}\right\} \tag{4}$$

where $\overline{\text{-}}$ is defined as follows for $f\colon k \to l$, $g\colon l \to m$, and $h\colon m \to n$.

$$\overline{\mathrm{id}_n} = \mathrm{id}_{2^n} \tag{5}$$

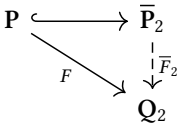
$$\overline{g \circ f} = \overline{g} \circ \overline{f} \tag{6}$$

$$\overline{f} \otimes \overline{h} \overset{\text{def}}{=} \overline{f + h} = s_{2^n,2^l} \circ (\underbrace{\overline{f} \oplus \overline{f} \oplus \cdots \oplus \overline{f}}_{2^n \text{ times}}) \circ s_{2^k,2^n} \circ (\underbrace{\overline{h} \oplus \overline{h} \oplus \cdots \oplus \overline{h}}_{2^k \text{ times}}) \tag{7}$$

Theorem 3. *The category* $(\overline{\mathbf{P}}, \otimes, 1, \oplus, 0)$ *is semisimple bipermutative.*

We are interested in objects in $\overline{\mathbf{P}}$ that are powers of 2. Given how generators in **P** are mapped into $\overline{\mathbf{P}}$, the embedding $\mathbf{P} \hookrightarrow \overline{\mathbf{P}}$ corestricts to an embedding $\mathbf{P} \hookrightarrow \overline{\mathbf{P}}_2$.

Corollary 4. *Given a controllable prop $(\mathbf{P}, +, 0, x)$, and a strict monoidal functor $F\colon \mathbf{P} \to \mathbf{Q}$ to a semisimple bipermutative category with $F(x) = \gamma_{1,1}$, there is a unique prop morphism $\overline{F}_2\colon \overline{\mathbf{P}}_2 \to \mathbf{Q}_2$ such that $\overline{F}_2$ preserves the NOT gate and the following diagram commutes.*



Theorem 5. *The category $\overline{\mathbf{X}}$ is exactly the category of permutations.*

We now redefine the functors $\alpha\colon \mathbf{cX} \to \overline{\mathbf{X}}_2$ and $\beta\colon \overline{\mathbf{X}}_2 \to \mathbf{cX}$ to fit the topic at hand.

3.1 Rig is control

$$
\begin{array}{rcl}
A\colon \quad \mathbf{cP} & \to & \overline{\mathbf{P}}_2 \\
n & \mapsto & 2^n \\
f \in \mathbf{cX} & \mapsto & \alpha(f) \\
g \in G & \mapsto & \overline{g} \\
C^1(f) & \mapsto & \mathrm{id}_{2^n} \oplus A(f) \\
C^0(f) & \mapsto & A(f) \oplus \mathrm{id}_{2^n} \\
\mathrm{id}_m + f & \mapsto & \mathrm{id}_{2^m} \otimes A(f)
\end{array}
\qquad
\begin{array}{rcl}
B\colon \quad \overline{\mathbf{P}}_2 & \to & \mathbf{cP} \\
2^n & \mapsto & n \\
f \in \overline{\mathbf{X}}_2 & \mapsto & \beta(f) \\
\overline{g} \in \overline{G} & \mapsto & g \\
\mathrm{id}_{2^n} \oplus f & \mapsto & C^1(B(f)) \\
f \oplus \mathrm{id}_{2^n} & \mapsto & C^0(B(f))
\end{array}
$$

Lemma 6. *The functors $A\colon \mathbf{cP} \to \overline{\mathbf{P}}_2$ and $B\colon \overline{\mathbf{P}}_2 \to \mathbf{cP}$ are well-defined prop morphisms.*

Both functors are well-defined and each other's inverse, yielding an isomorphism of props.

Theorem 7. *The props $\mathbf{cP}$ and $\overline{\mathbf{P}}_2$ are isomorphic.*

4 APPLICATIONS

To showcase the usefulness of the control equations of Figure 1, this section discusses five applications drawn from circuit theory, both Boolean and quantum, that can be handled easily using our control theory.

4.1 Sleator-Weinfurter

The Sleator-Weinfurter construction is a general construction for forming a doubly controlled f^2-gate using nothing but controlled f-gates and controlled NOT gates (see Figure 2). This property has led to the quantum synthesis of reversible circuits being studied by means of the NCV gate set $\{NOT, CV, CNOT\}$ (see, e.g., [1]). Originally shown through linear algebra [4], the construction has a simple proof in terms of the control equations.

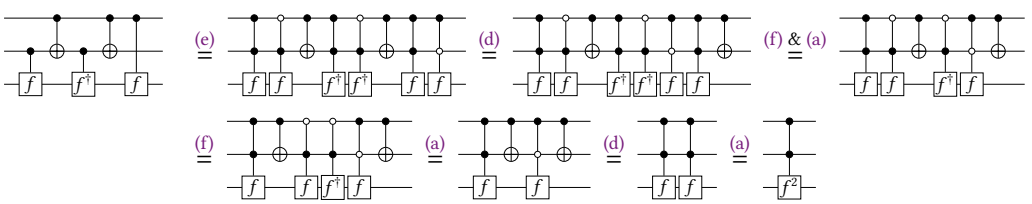


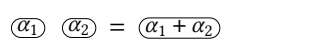
Fig. 2. Sleator-Weinfurter identity through control equations.

4.2 Quantum circuits

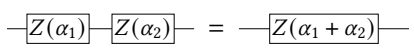
A complete equational theory for quantum circuits was an open question that was solved only recently [15] with several later improvements [13, 14, 18]. These papers already refer to some equations as *structural*. We show here that these equations are structural in a formal and categorical sense: they are only about control, and follow directly from the structure of a rig category.

Let $(\mathbf{Z}, +, 0)$ be the prop generated by $\alpha\colon 0 \to 0$ for $\alpha \in \mathbb{R}$, and $Z(\alpha)\colon 1 \to 1$ for $\alpha \in \mathbb{R}$, and $H\colon 1 \to 1$ satisfying

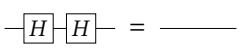
(8)



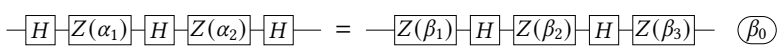
(9)



(10)

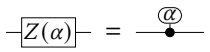


(11)



(12)

where (12) is the well-known Euler decomposition, in which β_0, β_1, β_2 and β_4 can be computed from α_1 and α_2 deterministically. We choose the crop $(\mathbf{Z}, +, 0, HZ(\pi)H)$ and can now form its controlled prop $\mathbf{cZ}$. Interestingly, the prop $\mathbf{cZ}$ is not immediately the prop of unitary operations: for a given α, the morphisms $C^1(\alpha)$ and $Z(\alpha)$ have the same semantics in unitaries but are still different in $\mathbf{cZ}$. We need to quotient further with the following equation:

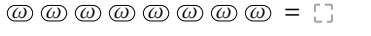


(13)

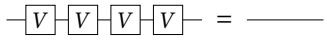
and we write $\mathbf{cZ}_{/\simeq}$ for this category. From this point, it is simple to show that we have equivalent equations to the complete equational theory for quantum circuits [18], and therefore $\mathbf{cZ}_{/\simeq}$ is isomorphic to the category of unitaries on qubits.

Theorem 8. *Equations* (8), (9), (10), (11), (12) *together with the control equations of Figure 1 and equation* (13)*, are sound and complete for quantum circuits.*

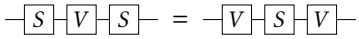
In fact, the same general strategy works to obtain a complete equational theory for quantum circuits formed from certain discrete gate sets by exploiting the rig structure shown in [10]. Let $(\mathbf{\Pi}, +, 0)$ be the prop generated by $\omega : 0 \to 0$, $V : 1 \to 1$, and $S : 1 \to 1$ satisfying



(14)

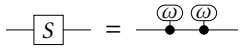


(15)



(16)

Choose now the crop $(\mathbf{\Pi}, +, 0, V^2)$, form its controlled prop $\mathbf{c\Pi}$, and quotient it further by the equation



(17)

to obtain the category $\mathbf{c\Pi}_{/\simeq}$. Recall that the *Gaussian Clifford+T* gate set [2] consists of the gates S, K, X, CX, and CCX, where $K = \frac{1-i}{\sqrt{2}}H$, and H is the usual Hadamard gate. We then obtain the desired result:

Theorem 9. *Equations* (14), (15), (16)*, together with the control equations of Figure 1 and equation* (17)*, are sound and complete for Clifford circuits, Clifford+T circuits with* ≤ 2 *qubits, and Gaussian Clifford+T circuits.*

REFERENCES

[1] N. Abdessaied, M. Amy, R. Drechsler, and M. Soeken. Complexity of reversible circuits and their quantum implementations. *Theoretical Computer Science*, 618:85–106, 2016.

[2] M. Amy, A. N. Glaudell, and N. J. Ross. Number-theoretic characterizations of some restricted clifford+T circuits. *Quantum*, 4:252, 2020.

[3] S. Balauca and A. Arusoaie. Efficient constructions for simulating multi controlled quantum gates. In *International Conference on Computer Science*, volume 13353 of *Lecture Notes in Computer Science*, pages 179–194. Springer, 2022.

[4] A. Barenco, C. H. Bennett, R. Cleve, D. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolin, and H. Weinfurter. Elementary gates for quantum computation. *Physical Review A*, 5:3457–3467, 1995.

[5] X. Bian and P. Selinger. Generators and relations for $U_n(\mathbb{Z}[\frac{1}{2}, i])$. In *Quantum Physics and Logic*, volume 343 of *Electronic Proceedings in Theoretical Computer Science*, pages 145–164, 2021.

[6] X. Bian and P. Selinger. Generators and relations for 2-qubit Clifford+T operators. *Electronic Proceedings in Theoretical Computer Science*, 394:13–28, 2023.

[7] A. Bisio, M. Dall'Arno, and P. Perinotti. Quantum conditional operations. *Physical Review A*, 94:022340, 2016.

[8] F. Bonchi, B. Sobociński, and F. Zanasi. Interacting Hopf algebras. *Journal of Pure and Applied Algebra*, 221(1):144–184, 2017.

[9] J. Carette, C. Heunen, R. Kaarsgaard, and A. Sabry. The quantum effect: A recipe for quantum-Π. In *Proceedings of the ACM on Programming Languages*, volume 8, pages 1–29, 2024.

[10] J. Carette, C. Heunen, R. Kaarsgaard, and A. Sabry. With a few square roots, quantum computing is as easy as Π. *Proceedings of the ACM on Programming Languages*, 8, 2024.

[11] J. Carette and A. Sabry. Computing with semirings and weak rig groupoids. In *European Symposium on Programming*, volume 9632 of *Lecture Notes in Theoretical Computer Science*, pages 123–148. Springer, 2016.

[12] Z. Chen, W. Liu, Y. Ma, W. Sun, R. Wang, H. Wang, H. Xu, G. Xue, H. Yan, Z. Yang, J. Ding, Y. Gao, F. Li, Y. Zhang, Z. Zhang, Y. Jin, H. Yu, J. Chen, and F. Yan. Efficient implementation of arbitrary two-qubit gates using unified control. *Nature Physics*, 21:1489–1496, 2025.

[13] A. Clément, N. Delorme, and S. Perdrix. Minimal equational theories for quantum circuits. In *Logic in Computer Science*, pages 27:1–27:14. ACM/IEEE, 2024.

[14] A. Clément, N. Delorme, S. Perdrix, and R. Vilmart. Quantum circuit completeness: Extensions and simplifications. In *Computer Science Logic*, volume 288 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 20:1–20:23, 2024.

[15] A. Clément, N. Heurtel, S. Mansfield, S. Perdrix, and B. Valiron. A complete equational theory for quantum circuits. In *Logic in Computer Science*, pages 1–13. ACM/IEEE, 2023.

[16] A. Clément and S. Perdrix. PBS-calculus: A graphical language for coherent control of quantum computations. In *Mathematical Foundations of Computer Science*, volume 170 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 24:1–24:14, 2020.

[17] A. Clément and S. Perdrix. Resource optimisation of coherently controlled quantum computations with the pbs-calculus. In *Mathematical Foundations of Computer Science*, volume 241 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 36:1–36:15, 2022.

[18] N. Delorme and S. Perdrix. Diagrammatic reasoning with control as a constructor, applications to quantum circuits, 2025. arXiv:2508.21756.

[19] J. M. Erbele. *Categories in control: applied PROPs*. PhD thesis, University of California, Riverside, 2016.

[20] W. Fang, C. Heunen, and R. Kaarsgaard. Hadamard-Π: Equational quantum programming. arXiv:2506.06835, 2025.

[21] D. R. Ghica and A. Jung. Categorical semantics of digital circuits. In *Formal Methods in Computer-Aided Design*, pages 41–48, 2016.

[22] C. Heunen and R. Kaarsgaard. Quantum information effects. *Proceedings of the ACM on Programming Languages*, 6, 2022.

[23] C. Heunen, R. Kaarsgaard, and L. Lemonnier. One rig to control them all, 2025. arXiv:2510.05032.

[24] R. Kaarsgaard. All you need is controlled-V: universality of a standard two-qubit gate by catalytic embedding. arXiv:2509.07578, 2025.

[25] M. L. Laplaza. Coherence for distributivity. In G. M. Kelly, M. Laplaza, G. Lewis, and Saunders Mac Lane, editors, *Coherence in Categories*, pages 29–65. Springer, 1972.

[26] S. M. Li, N. J. Ross, and P. Selinger. Generators and relations for the group $\mathrm{O}_n(\mathbb{Z}[1/2])$. In *Quantum Physics and Logic*, volume 343 of *Electronic Proceedings in Theoretical Computer Science*, pages 210–264, 2021.

[27] S. Mac Lane. Categorical algebra. *Bulletin of the American Mathematical Society*, 71:40–106, 1965.

[28] R. Sharma and S. Archour. Optimizing ancilla-based quantum circuits with SPARE. *Proceedings of the ACM on Programming Languages*, 9, 2025.

[29] V. V. Shende, S. S. Bullock, and I. L. Markov. Synthesis of quantum logic circuits. In *Asia and South Pacific Design Automation Conference*, pages 272–275. ACM, 2005.

[30] Y. Shi. Both Toffoli and controlled-NOT need little help to do universal quantum computing. *Quantum Information and Computation*, 3(1):84–92, 2003.
[31] T. Sleator and H. Weinfurter. Realizable universal quantum logic gates. *Physical Review Letters*, 74:4087–4090, 1995.
[32] M. K. Thomsen, R. Kaarsgaard, and M. Soeken. Ricercar: a language for describing and rewriting reversible circuits with ancillae and its permutation semantics. In *Reversible Computing*, pages 200–215, 2015.
[33] T. Toffoli. Reversible computing. In *International Colloquium on Automata, Languages, and Programming*, Lecture Notes in Computer Science, pages 632–644. Springer, 1980.
[34] H. Vollmer. *Introduction to circuit complexity*. Springer, 1999.
[35] D. Yau. *Bimonoidal Categories, E_n-Monoidal Categories, and Algebraic K-Theory: Volume I: Symmetric Bimonoidal Categories and Monoidal Bicategories*, volume 283 of *Mathematical Surveys and Monographs*. American Mathematical Society, 2024.
[36] N. Yu, R. Duan, and M. Ying. Five two-qubit gates are necessary for implementing the Toffoli gate. *Physical Review A*, 88:010304, 2013.